UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,705	04/02/2004	Tetsuharu Ohya	500.43733X00	9724

20457 7590 04/06/2007 ANTONELLI, TERRY, STOUT & KRAUS, LLP 1300 NORTH SEVENTEENTH STREET SUITE 1800 ARLINGTON, VA 22209-3873	**EXAMINER** LE, THU NGUYET T

ART UNIT	PAPER NUMBER
2162	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	10/815,705	OHYA ET AL.
	Examiner	Art Unit	
	Thu-Nguyet Le	2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>03 January 2007</u>.

2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1 and 3-19* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1 and 3-19* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>02 April 2004</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This office action has been issued in response to amendment file 03 January

2007. Claims 1, 3-19 are pending. Accordingly, this action has been made FINAL.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1, 4, 6-7, 11, 13, 15-16 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Serbinis et al. (US 6,584,466) in view of Fergus (US 2002/0077999).

With respect to claim 1, Serbinis discloses an information processing apparatus

supporting secret information management, comprising:

a management master extraction module which receives a management target

file containing secret information (figure 4, blocks 82, 83, column 9, lines 32-33) via an

input interface (column 15, lines 64-65) and extracts management master information,

including a file ID (column 7, line 62, "unique key/name") and information on validity of

the management target file (column 8, line 1, "active" and "delete"), from the

management target file;

a storage device which stores a file management database ("new document...

are stored to the DMS system", column 7, lines 52-54) with which the management

master information on each management target file is registered (column 7, line 50,

"document records are created in DMS database");

a storage event output module which outputs a signal indicating a storage event

of the management target file in the storage device to an output interface (figure 4,

block 86, column 9, lines 50-52, "notification message to authorized user informing that

the document in store");

a deletion target extraction module which receives a deletion request regarding

the management target file via the input interface and extracts information on the

management target file corresponding to the deletion request from the file management

database (column 8, line 18, document is requested to be deleted);

a management master information update module which updates the validity

information on the management target file deleted by the file deletion module, included

in the management master information registered with the file management database,

into invalid (column 8, line1, the state for a document instance is "deleted" which means

invalid); and

a deletion information output module which outputs a signal indicating that the

management target file has been deleted by the file deletion module to the output

interface (column 5, lines 66-67, column 6, line 1, "dispatches notifications...to users of

DMS system concerning the status of documents stored in the DMS system"); and

However, Serbinis does not implicitly disclose:

a mode determination module responsive to the deletion target extraction

module, which determines whether deletion mode information included in the delection

request indicates a seft-destructive mode requesting deletion of the management

master information as well as deletion of the management target file;

a file deletion module which executes the deletion of the management target file

from the storage device in response to a first determination result by the mode

determination module indicating that the deletion mode information does not indicate

the seft-destructive mode;

a management master information deletion module which locates the

management master information of the management target file which has been

registered with the file management database, and deletes the management master

information and the management target file in response to a second determination

result by the mode determination module indicating that the deletion mode information

indicates the self-destructive mode.

In the same field of endeavor, Fergus teaches system and method for

programmable removal of sensitive information from computing systems, wherein

receiving selections for removing sensitive information options, generating a purge

script file based on the selected information removal options. The purge is performed by

executing fo the purge script file (para.[0011] lines 4-8, fig.3 and 4).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made having the teachings of Serbinis and Fergus before him/her to

incorporate the system for programmable removal of sensitive information from

computing systems into the information processing apparatus supporting secret

information management to provide automatic initiation of removal of information, as

well as bypass protection against hostile entities attempting to circumvent the sensitive

information removal process. One of ordinary skill in the art would be motivated to make

the aforementioned combination with reasonable expectation of success.

Claim 4 is rejected for the reasons set forth hereinabove for claim 1 and

furthermore Serbinis teaches information processing apparatus, comprising:

an access authority extraction module which receives a usage request regarding

a management target file via the input interface (column 9, lines 66-67, "Authorized

user may then request retrieval of the document form store") and extracts access

authority information on the management target file corresponding to the usage request

from the file management database (figure 2, block 61 "Document information" and

"Rights (document and document group)", column 10, lines);

an access authority judgment module which receives user authority information

on a user corresponding to the usage request via the input interface (figure 2, block 62

"name and logon information") and judges whether the management target file

corresponding to the usage request may be accessed or not by checking the user

authority information with the access authority information (column 10, lines 12-13,

"whether authorized user has rights to get or check out a document depends upon the

access rights granted");

an available file output module which extracts the management target file

corresponding to the usage request from the storage device and outputs the extracted

management target file to the output interface if the access authority judgment module

judged that the management target file may be accessed (figure 4, block 90 "Authorized

user receives document form internet store");

an updated file generation module which receives an update process for

updating the management target file outputted by the available file output module via

the input interface and thereby generates an updated file (column 10, lines 18-19, "an

Authorized user has checked out and modified the document"); a

an updated file storage module which stores the updated file in the storage

device (column 10, line 19, "check in the modified document to the DMS system"); and

an updated file registration module which extracts management master

information on the updated file and stores the extracted management master

information in the file management database (column 10, lines 21-22, "new version

identifier in the document tables of DMS database").

Claim 6 is rejected for the reasons set forth hereinabove for claims 1, 4 and

furthermore Serbinis teaches information processing apparatus, comprising:

a relevant deletion target extraction module which extracts information on the

updated file derived from the management target file corresponding to the deletion

request (column 8, line 18) in addition to the information on the management target file

from the file management database;

a relevant file deletion module which executes the deletion of the updated file

from the storage device based on the information on the updated file extracted by the

relevant deletion target extraction module (column 8, lines 19-20, "the physical file

corresponding to the document instance is removed/deleted from storage");

a relevant management master information update module which updates the

validity information on the updated file deleted by the relevant file deletion module,

included in the management master information registered with the file management

database, into invalid (column 8, line1, "deleted" means invalid); and

an informing module which informs a second information processing apparatus

connected with the information processing apparatus via a network that the updated file

has been deleted by the relevant file deletion module, via the output interface (column

5, lines 66-67, column 6, line 1, "dispatches notifications...to users of DMS system

concerning the status of documents stored in the DMS system").

Claim 7 is rejected for the reasons set forth hereinabove for claim 1 and

furthermore Serbinis teaches an information processing apparatus, comprising:

a business application process judgment module which judges whether a user

has authority or not in a business process authority database, in which the

presence/absence of deletion authority, backup authority or usage authority of each

user regarding each management target file is stipulated, when a business application

using a management target file is executed (figure 2, block 62, "Name and login

information", column 9, lines 26-31, the specific access rights granted to each

authorized user are recorded in the document tables of DMS database. Different users

may be granted different access right); and

a business application process execution module which extracts the

management target file to be processed by the business application from the storage

device and provides the management target file to the business application if the

business application process judgment module judged that the user has the deletion

authority, the backup authority or the usage authority regarding the management target

file (column 9, lines 26-31, user can access, review, modify document basing on

specified access rights granted to each user) .

Claims 11, 13, 15-16 are rejected on grounds corresponding to the reasons

given above for claims 1, 4, 6-7 because claims 11, 13, 15-16 claim equivalent

limitations as claims 1, 4, 6-7.

4.   Claims 3, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Serbinis et al. (US 6,584,466) in view of Fergus (US 2002/0077999) and further in view

of Johnson (US 7,080,260).

Claim 3 is rejected for the reasons set forth hereinabove for claim1.

Serbinis does not explicitly teaches information processing apparatus, comprising:

an access authority extraction module which receives a backup request

regarding a management target file via the input interface and extracts access authority

information on the management target file corresponding to the backup request from the

file management database;

an access authority judgment module which receives user authority information

on a user corresponding to the backup request via the input interface and judges

whether the management target file corresponding to the backup request may be

accessed or not by checking the user authority information with the access authority

information;

a copy generation module which extracts the management target file corresponding to the backup request from the storage device and generates a copy file of the management target file if the access authority judgment module judged that the management target file may be accessed;

a copy output module which outputs the copy file of the management target file to a backup medium; and

a copy file registration module which extracts management master information on the copy file and stores the extracted management master information in the file management database.

However, Johnson teaches a system to archive and retrieve data files wherein an access authority extraction module which receives a backup request regarding a management target file via the input interface (column 5, line 11) and extracts access authority information on the management target file corresponding to the backup request from the file management database (column 5, lines 36-38, 42, once user has logged on the server using user's password and been verified via second software as an authorized user. It is inherently authority information of the file is extracted and used in order to verify authorized user);

an access authority judgment module which receives user authority information on a user corresponding to the backup request via the input interface (column 5, line 23, "logon password") and judges whether the management target file corresponding to the backup request may be accessed or not by checking the user authority information with

the access authority information (column 5, lines 37-38, "verified ... as an authorized

user");

a copy generation module which extracts the management target file

corresponding to the backup request from the storage device and generates a copy file

of the management target file if the access authority judgment module judged that the

management target file may be accessed (figure 2, bock 34 "files ... are backed up");

a copy output module which outputs the copy file of the management target file to

a backup medium (figure 2, bock 38 "data stored", column 5, lines 57-58); and

a copy file registration module which extracts management master information on

the copy file and stores the extracted management master information in the file

management database (figure 2, block 61 "Document Information" and "Information on

document instance").

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to incorporate the system to archive and retrieve encrypted data

files as disclosed by Johnson into the information processing apparatus as disclosed in

Serbinis to utilize encryption/decryption and code recognition technology associated

with Secure Agent (column 1, lines 39-40) so that backup files are efficiently managed

in order to improve protection of secret, classified information. One of ordinary skill in

the art would be motivated to make the aforementioned combination with reasonable

expectation of success.

Claim 12 is rejected on grounds corresponding to the reasons given above for

claims 3 because claim 12 claims equivalent limitations as claim 3.

5.   Claims 5, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Serbinis et al. (US 6,584,466) in view of Fergus (US 2002/0077999) and further in view

of Boneh et al. (US 6,134,660).

Claim 5 is rejected for the reasons set forth hereinabove for claim 3.

Serbinis does not explicitly teaches information processing apparatus, comprising:

a relevant deletion target extraction module which extracts information on the

copy file derived from the management target file corresponding to the deletion request

in addition to the information on the management target file from the file management

database;

a relevant file deletion module which executes the deletion of the copy file from

the backup medium based on the information on the copy file extracted by the relevant

deletion target extraction module;

a relevant management master information update module which updates the

validity information on the copy file deleted by the relevant file deletion module, included

in the management master information registered with the file management database,

into invalid; and

an informing module which informs a second information processing apparatus

connected with the information processing apparatus via a network that the copy file

has been deleted by the relevant file deletion module, via the output interface.

However, Boneh discloses a method that enables a user to remove a file form a file

system and from all back up tapes (abstract, lines 1-2). The "remove-file" command

instructs the computer system to delete a file (column 1, lines 53-54). Additional,

operator has to remove the data from many backup tapes (column 2, lines 27).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to incorporate the method as disclosed by Boneh into the

information processing apparatus as disclosed in Serbinis to erase all copies of

particular files, such as sensitive, confidential information (column 1, lines 39-40) in

order to increase security of protected information. One of ordinary skill in the art would

be motivated to make the aforementioned combination with reasonable expectation of

success.

  Claim 14 is rejected on grounds corresponding to the reasons given above for

claims 5 because claim 14 claims equivalent limitations as claim 5.

6. Claims 8-10, 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Serbinis et al. (US 6,584,466) in view of Fergus (US 2002/0077999) and further in

view of Capps (US 6,397,311).

  Claim 8 is rejected for the reasons set forth hereinabove for claim1.

  Serbinis does not explicitly teaches information processing apparatus,

comprising:

  a first copy execution module which copies information stored in the storage

device into a second storage device after the deletion of the management target file

from the storage device is executed by the file deletion module

  a first demagnetization execution module which writes a prescribed data pattern

to each memory unit of the storage device for a preset number of times;

a second copy execution module which copies the information stored in the

second storage device back into the storage device; and

a second demagnetization execution module which writes a prescribed data

pattern to each memory unit of the second storage device for a preset number of times.

However, Capps teaches a method of defragmenting a file system. After files are

deleted in a file system, the free spaces on the disk space become fragmented (column

1, lines 14, 16-17). The method comprises copying all of the files to another medium,

such as a tape drive. After coping, they are deleted from the file system. A utility

program is run to rebuild the list of free space on the disk. The files are then copied

back onto the file system (column 1, lines 29-33)

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to incorporate the method for defragmenting as disclosed by Capps

into the information processing apparatus as disclosed in Serbinis to rearrange the file

segments and free space on the disk so that each file resides in a contiguous region on

the disk resulting in increased performance (column 1, lines 23-26). One of ordinary

skill in the art would be motivated to make the aforementioned combination with

reasonable expectation of success.

Claims 9, 10 are rejected for the reason discussed related to claim 8. Since

claim 8 is substantially equivalent to claims 9, 10.

Claims 17-19 are rejected on grounds corresponding to the reasons given above

for claims 8-10 because claims 17-20 claim equivalent limitations as claims 8-10.

Response to Amendment

7.   The claims have been amended to overcome 35 U.S.C. 112 2nd rejection.

Therefore, the claim rejection 35 U.S.C. 112 2nd has been removed.

8.   Applicants' argument regarding the 102(b) rejection based upon Serbinis for the

newly amended claim 1 has been considered.

With respect to applicants' argument at Serbinis does not disclose limitations

sensitive electronic files to be either perfectly deleted or imperfectly deleted basing upon

deletion mode. The argument is persuasive. The rejection for this limitation based upon

Serbinis is withdrawn.

However, the examiner respectfully submits Fergus' reference, which discloses

the sensitive electronic files to be either perfectly deleted or imperfectly deleted basing

upon deletion mode. The examiner refers applicants to the rejection supra. Fergus

discloses a system for programmable removal of sensitive information from computer

system, wherein sensitive information is deleted depending on selected options. Either

sensitive file is deleted or sensitive file and its other information are deleted (Fig.3, 4

and para.[0011] lines 4-8).

Accordingly, examiner strongly believes that a prima facie case has been clearly

establish with respect to the prior art rejection of the instant claims, given their broadest

reasonable interpretation.

Conclusion

9.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

·CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the ·

examiner should be directed to Thu-Nguyet Le whose telephone number is 571-270-

1093. The examiner can normally be reached on 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, John Breene can be reached on 571-272-4170. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. ·

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic
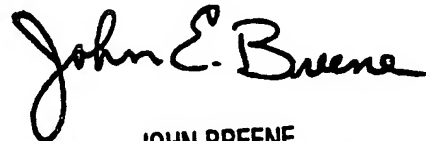
Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

T L

Thu-Nguyet Le   KBP
March 26, 2007

JOHN BREENE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100